Doc Code: AP.PRE.REQ

RECEIVED
CENTRAL FAX CENTER
SEP 14 2007

PTO/SB/33 (07-05)
Approved for use through xx/xx/200x. OMB 0651-00xx
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Docket Number (Optional)	
SCS-550-619	

Application Number	Filed
10/527,812	June 14, 2005
First Named Inventor	
Evrard	
Art Unit	**Examiner**
2196	K. Vicary

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ Applicant/Inventor

☐ Assignee of record of the entire interest. See 37 C.F.R. § 3.71. Statement under 37 C.F.R. § 3.73(b) is enclosed. (Form PTO/SB/96)

☒ Attorney or agent of record 27,393 (Reg. No.)

☐ Attorney or agent acting under 37CFR 1.34.
Registration number if acting under 37 C.F.R. § 1.34 _____

Signature

Stanley C. Spooner
Typed or printed name

703-816-4028
Requester's telephone number

September 14, 2007
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.*

☒ *Total of 1 form/s are submitted.

STATEMENT OF ARGUMENTS IN SUPPORT OF PRE-APPEAL BRIEF REQUEST FOR REVIEW

The following listing of clear errors in the Examiner's rejection and his failure to identify essential elements necessary for a *prima facie* basis of rejection is responsive to the Final Official Action mailed May 14, 2007 (Paper No. 20070507).

1. General differences between the claimed invention and the Qiu reference (U.S. Patent 6,804,782)

The present invention relates to providing data processing systems which manipulate secure data and at the same time maintain a high degree of security (Background of the Invention, specification, page 1).

As discussed in detail in Applicants' previously filed Amendment (filed April 17, 2007, pages 11 and 12), there is a common problem of preventing the characteristic power consumption signature associated with a write to a data processing register indicating that a write has taken place. The Qiu reference solves the problem by masking the characteristic power signature by performing an algorithm producing a significant increase in activity within the power signature, thereby masking any changes which occur as a result of the conditional write data processing operation. As will be seen, Qiu's provision of an algorithmic solution for generating masking power usages is a known manner of defeating the so-called simple power analysis (SPA).

However, the present invention represents a subsequent generation of security defense and focuses on the intrinsic weaknesses of an encryption algorithm. Such weaknesses may be undetectable by way of an SPA and yet may still be detected by using differential power analysis (DPA). The presently claimed invention recognizes that, even on the level of single instructions

being executed by a processor core, there is still a detectable change in power usage where data is written to a particular register and where data is not written to a register.

Qiu's attempts to mask this power usage difference is simply a different approach from Applicants' invention which utilizes a "trash register" and writes a result data value to the trash register when the condition codes do not permit a write to effect a change in the processor core. While the Qiu device overcomes a simple power analysis (SPA), it can be defeated by using a differential power analysis (DPA). The presently claimed invention addresses the same problem addressed in Qiu, but not only defeats SPA, but differential power analysis (DPA) as well.

2. Error #1 – Applicants' appealed from independent claim 1 specifically recites a "trash register" and the Examiner addresses this in the first full paragraph on page 3 of the Official Action

Unfortunately, the Examiner does not identify any structure disclosed in the Qiu reference which comprises the claimed "trash register." Accordingly, Qiu cannot anticipate or render obvious the subject matter of independent claim 1 or claims dependent thereon.

3. Error #2 – In addition to the "trash register," independent claim 1 also requires that the interconnection such that "a result data value will be written instead of a data processing register upon execution of said conditional-write data processing instruction . . ."

The Examiner has not indicated any interrelationship between the non-identified "trash register" which he presumably believes is present in Qiu and the fact that result data values are written to the trash register instead of a data processing register. Because anticipation requires all elements "arranged as in the claim," the anticipation rejection also fails for lack of this claimed interrelationship. Again, the claim language appears to be controlling and the last paragraph in claim 1 specifies writing the result data value to the trash register "when said

condition codes within said conditional-write data processing instruction do not permit a write to effect a change in state of said processor core." Thus, depending upon the "conditional-write data processing instruction," the instruction will either write to "a data processing register" or to the claimed "trash register."

The claimed interrelationship between the claimed trash register and the claimed data processing registers is simply not disclosed in the Qiu reference and therefore there is clearly no support for a rejection of independent claim 1 or claims dependent thereon in view of the Qiu reference.

4. Error #3 – The Examiner fails to appreciate that the Qiu reference teaches away from the claimed invention by requiring an unnecessary mathematical operation

The cryptographic algorithm of Qiu carries out a number of mathematical operations, with the necessity of performing these operations being dependent on values in a private key. Where a particular mathematical operation is not needed, Qiu teaches performing an unnecessary mathematical operation in order to mask the presence or absence of the particular mathematical operation. This is shown in Qiu's Figure 3 and described at column 4, lines 21-35. It will be appreciated that in the "normal" portion of the cryptographic algorithm (step 300) where mathematical operations are "necessary," the data processing apparatus of Qiu will execute various instructions in order to carry out the algorithm.

As stated in Qiu, "while the algorithm is being implemented" (at column 4, line 27), when it is established that an operation is not required (by checking the key at step 304) an unnecessary mathematical operation and store to memory are performed (steps 308 and 312). The algorithm represented by Figure 3 will involve many distinct instructions being carried out by the data processing apparatus. Therefore, instead of Qiu teaching the claimed subject matter,

i.e., directing the result data value to be stored either in a "data processing register" if storage is desired or in the "trash register" if the data is not desired, Qiu merely requires the performance of an algorithm which includes an unnecessary mathematical operation. Qiu simply fails to disclose any concept of a single instruction being executed in one of two different ways as claimed in Applicants' independent claim 1.

Because Qiu teaches the sufficiency of a different solution to the problem (even though, as noted above, Qiu's solution does not prevent differential power analysis (DPA)), Qiu actually would lead one of ordinary skill in the art away from Applicants' claimed apparatus and the claimed interrelationship between apparatus elements. Because Qiu teaches away from the claimed invention, this evidences the non-obviousness of Applicants' claimed combination and any further rejection of claim 1 or claims dependent thereon is respectfully traversed.

5. Error #4 – The Examiner appears to misunderstand the language of claim 1 with respect to the meaning of the word "instruction"

The Examiner seems to be attempting to interpret the word "instruction" to cover whole sections of algorithmic procedure. This interpretation is inconsistent with the discussion in Qiu, specifically Figures 8 and 10.

Figure 8 illustrates a section of example code, showing how the Qiu algorithm is implemented. Note in particular the steps 7-9 which show what happens when a "0" is encountered in the key (described at column 7, lines 23-29), which is when Qiu teaches performing the unnecessary mathematical operation (see also column 3, lines 55-56 and step 304 of Figure 3). It will be noted that at step 7, Qiu requires a subroutine MonPro is called. This subroutine is illustrated in Figure 10 and described at column 7, lines 39-49. This subroutine involves the execution of many instructions. In light of the known and conventional

understanding of "instruction" as set out in Applicants' specification and known to those of ordinary skill, it is clear that Qiu is not concerned with events occurring at the instruction level and rather is concerned with events at the algorithm level. The Examiner also attempts to consider that a zero occurring in a private key (which the Examiner considers to be a "condition code"), the entire "MonPro" subroutine in Figure 10 is called into play. Those having even rudimentary skill in this art would not consider this to be a condition code which is encoded in an instruction to determine how that instruction is to be executed.

While the Examiner appears to be citing various portions of the Qiu reference which he believes disclose the claimed subject matter, a detailed analysis illustrates that the Qiu reference has nothing to do with Applicants' claimed invention. The fact that the Examiner misunderstands and/or misapplies the terms in the claim further evidences the inability of the Examiner to establish a *prima facie* case of either anticipation or obviousness.

SUMMARY

Based upon the final rejection, it is not clear that the Examiner understands the prior art or the claimed invention. There is no basis for an anticipation or obvious rejection where the primary reference Qiu fails to teach at least one claimed element (the "trash register") and at least one claimed interrelationship between elements (moving the data value to either the processor register or the trash register). Additionally, the Examiner seems to ignore that Qiu teaches away from the claimed invention.

As a result of the above, there is simply no support for the rejection of Applicants' independent claim 1 or claims dependent thereon under 35 USC §102 and/or §103. Applicants respectfully request that the Pre-Appeal Panel find that the application is allowed on the existing claims and prosecution on the merits should be closed.